

CLAIMS

1. A method of protecting sensitive data against use of a routine operating on said data, characterized in that it includes an operation of verifying the identity of each software task calling said routine (400), which operation is implemented by said routine.

2. A protection method according to claim 1, characterized in that said verification operation (400) includes an operation of reading an identifier of said task (304) and an operation of comparing (305) said identifier with predetermined identifiers.

3. A protection method according to either claim 1 or claim 2, characterized in that each routine operating on said data implements said verification operation (400).

4. A device for protecting sensitive data against use of a routine operating on said data, characterized in that it includes a verification system (104, 105, 106) adapted to verify the identity of each software task calling said routine, said verification system being implemented by said routine.

5. A protection device according to claim 4, characterized in that said verification system (104, 105, 106) includes a reading system (104, 105, 106) for reading an identifier of said task and a comparator system (104, 105, 106) for comparing said identifier and predetermined identifiers.

6. A protection device according to either claim 4 or claim 5, characterized in that each routine operating on said data implements said verification system (104, 105, 106).

7. A franking machine (1), characterized in that it includes a device according to any of claims 4 to 6.